Pilot Contamination Attack Detection and Defense Strategy in Wireless Communications

Ning Gao, Zhijin Qin, Xiaojun Jing

***Abstract*—In the channel training phase, the attacker launches a pilot contamination attack by sending a synchronized and identical pilot signal with the legitimate transmitter. Such an attack can contaminate the channel estimation and alter the legitimate beamformer design. In this letter, we propose a pilot contamination attack detection scheme and defense strategy for wireless communications. By considering the prior uncertainty of the attack, we find that the decision-maker will conservatively decide the state of the attack, which is a subjective choice. In this case, we derive the subjective detection probability, the subjective false alarm probability, and the threshold. We analyze the tradeoff problem between the ergodic wiretap channel rate and the subjective detection probability. Furthermore, based on the worst case that the attacker adopts the optimal power allocation to launch the optimal attack, we discuss the defense strategy of the optimal attack. Simulations show that the proposed scheme has a better performance than the benchmark method.**

***Index Terms*—Pilot contamination attack, defense strategy, wireless communications.**

I. Introduction

BEAMFORMING can be used to increase the signal power and enhance the communication security. Generally, beamformer is designed based on the channel state information (CSI), which is mainly estimated over the uplink channel [1], [2]. However, a pilot contamination attacker can actively send the pilot signal to the receiver, which is identical to the one from the transmitter to the receiver [3]. The channel training phase will be contaminated and the beamformer design is then altered. In this case, the beamformer designed by the transmitter could cause serious power leakage and degrade the channel secrecy rate.

The concept of pilot contamination attack was first introduced in [3], whereafter, there have been some work on this topic [4]–[8]. Yuan *et al.* [4] has proposed to add a random sequence to the pilot sequence, which makes it more difficult for the attackers to learn the pilot sequence. The code-frequency block group coding based pilot authentication has been proposed in [5] to separate the spoofer with high accuracy. Tugnait *et al.* [6] has superimposed a random sequence on the training sequence and proposed a source enumeration method to detect pilot contamination attack. As an extension of [6], [7] has improved it via estimation of legitimate and illegitimate channels, which further remits the impacts of the pilot spoofing. However, these work requires the modification of the training sequence structure, which limits their compatibility with the existing wireless systems. In terms of the spoofing power optimization, Zhou *et al.* in [3] have investigated how an eavesdropper can improve its eavesdropping performance via pilot contamination attack and have analyzed an optimal power allocation for eavesdropper. An energy ratio detector (ERD) without modifying the training sequence has been proposed in [8] to detect such an attack, in which the tradeoff problem between the eavesdropper's power and the detection performance has been investigated but the closed-form expression is still missing.

In this letter, we propose the receive power-to-noise ratio (RPNR) based pilot contamination attack detection scheme, which needs no prior information about the CSI and the noise, and requires no modification to the training sequence structure. With considering the prior uncertainty of the attack, the closed-form expression for the subjective detection probability, the subjective false alarm probability, and the threshold are derived. Moreover, the attacker's optimal power allocation is derived, and the defense strategy is discussed based on the optimal attack.

Notation: Boldface letter denotes matrix, such as $\mathbf{A}$. $\mathbf{A}^H$ is the Hermitian transpose of $\mathbf{A}$ and $\mathbf{R}_{\mathbf{A}}$ is the covariance matrix of $\mathbf{A}$. $\mathbf{I}_M$ is the identity matrix of dimension $M \times M$. The abbreviation i.i.d. denotes "independent and identically distributed". $\mathbb{E}\{\cdot\}$ denotes the expectation operator and $\mathbb{C}^{m\times n}$ denotes the complex space of matrix of dimension $m \times n$.

II. System Model and Problem Formulation

In the considered networks, the time-division duplex (TDD) is adopted and there are three components, including a legitimate transmitter Alice, an intended receiver Bob, and a pilot contamination attacker Eve. Alice is a base station equipped with M_T transmit antennas, while Bob and Eve are resource-limited devices with a single antenna, respectively. Denote $x_p(t)$ as the continuous time unit-energy pilot signal and $\mathbf{x}_p^N$ as the pilot signal with N samples. The channel between transmitter and receiver is denoted as $\mathbf{h}_{tr}, t, r \in \{A, B, E\}, t \neq r$, which follows zero-mean complex Gaussian process of unit-variance, i.e., $\mathbf{h}_{tr} \sim \mathcal{CN}(0, \mathbf{I}_{M_T})$. In the reverse training, the pilot signal received at Alice is given by

$$\mathbf{Y}_A = \sqrt{\mathcal{P}_B}\mathbf{h}_{BA}\mathbf{x}_p^N + \Phi\sqrt{\mathcal{P}_E}\mathbf{h}_{EA}\mathbf{x}_p^N + \mathbf{N}, \tag{1}$$

N. Gao is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China and also with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China, (e-mail: ngao@bupt.edu.cn).

Z. Qin is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K., (email: z.qin@qmul.ac.uk).

X. Jing is with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China, (e-mail: jxiaojun@bupt.edu.cn).

where $\mathbf{Y}_A \in \mathbb{C}^{M_T \times N}$, and the channel $\mathbf{h}_{BA}$, $\mathbf{h}_{EA} \in \mathbb{C}^{M_T \times 1}$. $\Phi \in \{0,1\}$ represents the absence and the presence of the attacker, respectively, and $\mathcal{P}_B$ and $\mathcal{P}_E$ are the power budget for Bob and Eve, respectively. $\mathbf{N} \in \mathbb{C}^{M_T \times N}$ is the i.i.d. additive white Gaussian noise (AWGN), in which each entry is with zero-mean and variance σ^2. Alice adopts maximum ratio transmission scheme to design the beamforming vector $\mathbf{w}$ as

$$\mathbf{w} = \frac{\hat{\mathbf{h}}_{AB}^{\Phi}}{\parallel \hat{\mathbf{h}}_{AB}^{\Phi} \parallel}, \tag{2}$$

where $\hat{\mathbf{h}}_{AB}^{\Phi}$ is the linear minimum mean square error (LMMSE) estimation of $\mathbf{h}_{AB}$ with i.i.d. normalized estimation error $\mathbf{h}_e^{\Phi} \sim \mathcal{CN}(0, \frac{\sigma_{\Phi}^2}{N}\mathbf{I}_{M_T})$ and $\parallel \cdot \parallel$ denotes the Euclidean norm. The LMMSE estimation of $\hat{\mathbf{h}}_{AE}$ is given by [9]

$$\hat{\mathbf{h}}_{AE} = \sqrt{\frac{\mathcal{P}_E}{\mathcal{P}_B}}\hat{\mathbf{h}}_{AB}^{1}. \tag{3}$$

In the downlink transmission, the N sampled data signal $\mathbf{x}_d^N$ received at Bob and Eve are given by

$$\mathbf{y}_B = \sqrt{\mathcal{P}_A} \parallel \hat{\mathbf{h}}_{AB}^{1} \parallel \mathbf{x}_d^N + \sqrt{\mathcal{P}_A}\mathbf{h}_e^{1\,H}\mathbf{w}\mathbf{x}_d^N + \mathbf{n}, \tag{4}$$

$$\mathbf{y}_E = \sqrt{\frac{\mathcal{P}_A\mathcal{P}_E}{\mathcal{P}_B}} \parallel \hat{\mathbf{h}}_{AB}^{1} \parallel \mathbf{x}_d^N + \sqrt{\mathcal{P}_A}\tilde{\mathbf{h}}_e^{1\,H}\mathbf{w}\mathbf{x}_d^N + \mathbf{n}, \tag{5}$$

respectively, where $\mathcal{P}_A$ is the power budget for Alice, $\mathbf{n} \in \mathbb{C}^{1\times N}$ is the AWGN and $\tilde{\mathbf{h}}_e^{1} \sim \mathcal{CN}(0, \frac{\tilde{\sigma}_1^2}{N}\mathbf{I}_{M_T})$ is the estimation error at Eve with $\tilde{\sigma}_1^2 = \frac{\mathcal{P}_E}{\mathcal{P}_B}\sigma_1^2$.

III. Pilot Spoofing Attack Detection

The pilot contamination attack can cause a power leakage at the receiver. Since the CSI and the noise are unknown, it is hard to detect the attack roughly via the receive signal power, especially when the channel environment is worse. Therefore, we propose the following detection scheme.

In the downlink transmission, the data with N number of samples is received at Bob, and the sampled covariance matrix is calculated as $\mathbf{R}_{\mathbf{y}_B} = \mathbb{E}\{\mathbf{y}_B^H\mathbf{y}_B\}$. Then, the sampled covariance matrix $\mathbf{R}_{\mathbf{y}_B}$ is written in a diagonal form

$$\mathbf{E}^H\mathbf{R}_{\mathbf{y}_B}\mathbf{E} = \mathrm{diag}(\underbrace{\lambda_1+\sigma^2,\cdots,\lambda_k+\sigma^2}_{\text{signal+noise}},\underbrace{\sigma^2,\cdots,\sigma^2}_{\text{noise}}), \tag{6}$$

where $\mathbf{E}$ is the orthonormal matrix corresponding to the eigenvalue vector. Note that if the eigenvalues are arranged in the descending order, i.e., $\lambda_1+\sigma^2 \geq \cdots \geq \lambda_k+\sigma^2 > \sigma^2 = \cdots = \sigma^2$, the signal power is concentrated on the first k eigenvalues. Thereby, we utilize the maximum eigenvalue to minimum eigenvalue ratio to detect the attacker. The detection problem is formulated as the following hypothesis test

$$\frac{\lambda_{max}}{\lambda_{min}} = \frac{\lambda_1+\sigma^2}{\sigma^2} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \mathscr{T}, \tag{7}$$

where $\mathcal{H}_0$ indicates the attacker is absent and $\mathcal{H}_1$ indicates the attacker is present. If the test statistic is less than a threshold $\mathscr{T}$, the decision-maker (Bob) accepts the hypothesis $\mathcal{H}_1$, otherwise, it accepts $\mathcal{H}_0$.

A. Subjective Detection Probability & False Alarm Probability

Note that λ_{max} consists of the majority of the signal power in $\mathbf{y}_B$ and λ_{min} represents the variance of AWGN, however, they are hard to express via a closed-form expression. Hence, we transform (7) into the following hypothesis test

$$\frac{\parallel \mathbf{y}_B \parallel^2}{\lambda_{min}} = \frac{\mathcal{P}_A \parallel \hat{\mathbf{h}}_{AB}^{\Phi} \parallel^2 + \mathcal{P}_A \parallel \mathbf{h}_e^{\Phi\,H}\mathbf{w} \parallel^2}{\sigma^2} + 1 \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \gamma, \tag{8}$$

where the threshold γ can be denoted by threshold $\mathscr{T}$, namely $\gamma = \frac{N[\sigma^2(\mathscr{T}+N-1)+\lambda_2+\cdots+\lambda_k]}{\sigma^2}$. Since $\mathbf{w}$ is a unitary matrix, $\mathbf{h}_e^{\Phi\,H}\mathbf{w}$ has the same distribution as $\mathbf{h}_e^{\Phi\,H}$, i.e., when $\Phi = 1$, $\mathbf{h}_e^{1\,H}\mathbf{w} \sim \mathcal{CN}(0, \frac{\sigma_1^2}{N})$ [10]. From the strong law of large numbers, for N sampled data signal, $P(\lim_{N\to\infty} \parallel \mathbf{h}_e^{\Phi\,H}\mathbf{w} \parallel^2 = \sigma_{\Phi}^2) = 1$ [9, 7B.2]. Let $\varphi_{\Phi} = \parallel \hat{\mathbf{h}}_{AB}^{\Phi} \parallel^2$, we can rewrite (8) as

$$\frac{\parallel \mathbf{y}_B \parallel^2}{\lambda_{min}} = \frac{\mathcal{P}_A\varphi_{\Phi} + \mathcal{P}_A\sigma_{\Phi}^2}{\sigma^2} + 1. \tag{9}$$

When making a decision with prior uncertainty, the conservative subjective choice reflects the real-life decision [11]. The subjective probability is to model the objective probability[1] P, which is given by

$$P^s = \exp\big(-(\ln\frac{1}{P})^{\mu_s}\big). \tag{10}$$

The function P^s is the subjective probability, which is S-shaped and asymmetrical, and the subjective parameter $\mu_s \in (0,1]$ reveals how subjective choice distorts the probability P.

Theorem 1: With considering the prior uncertainty of the attack, the decision-maker in (7) is conservative, which can subjectively distort the objective probability.

Proof: We assume the prior probabilities of the attack presence and absence are $P(1), P(0)$ and the objective probabilities are P_d, P_f. From the law of total probability, the real-life probabilities can be denoted by $P_d^s = P(1)P_d$ and $P_f^s = P(0)P_f$. The probability $P_{d(f)}^s \leq P_{d(f)}$ suggests the choice of decision-marker is conservative under the prior uncertainty, which subjectively distorts the objective probability. ■

Whereas, $P(1), P(0)$ is unknown in practice, we use the subjective probability in (10) to model the real-life performance of the RPNR. The subjective false alarm probability is defined as

$$\begin{aligned} P_f^s &= \exp\left(-\left(\ln\frac{1}{Pr\left(\frac{\mathcal{P}_A\varphi_0+\mathcal{P}_A\sigma_0^2}{\sigma^2}+1<\gamma\right)}\right)^{\mu_s}\right) \\ &= \exp\left(-\left(\ln\frac{1}{F_0(\gamma)}\right)^{\mu_s}\right), \end{aligned} \tag{11}$$

where $Pr(\cdot|\cdot)$ is the conditional probability. Similarly, the subjective detection probability is defined as

$$P_d^s = \exp\left(-\left(\ln\frac{1}{F_1(\gamma)}\right)^{\mu_s}\right), \tag{12}$$

where $F_{\Phi}(\cdot), \Phi \in \{0,1\}$ are the cumulative distribution

[1]To distinguish the term "subjective", we use the term "objective" to name the detection probability and false alarm probability in detection theory.

functions of the sum of i.i.d. exponential distribution, which follows the Gamma distribution $\varphi_\Phi \sim \Gamma(NM_T, 1-\frac{\sigma_\Phi^2}{N})$. The objective false alarm probability is given by

$$\begin{aligned} F_0(\gamma) &= Pr\left(\frac{\mathcal{P}_A\varphi_0+\mathcal{P}_A\sigma_0^2}{\sigma^2}+1<\gamma\right) \\ &= Pr\left(\varphi_0<\frac{(\gamma-1)\sigma^2-\mathcal{P}_A\sigma_0^2}{\mathcal{P}_A}\right) \\ &= \frac{\Gamma(NM_T, z_0\beta_0)}{\Gamma(NM_T)}, \end{aligned} \tag{13}$$

where $z_0 = \frac{(\gamma-1)\sigma^2-\mathcal{P}_A\sigma_0^2}{\mathcal{P}_A}$, $\beta_0 = 1-\frac{\sigma_0^2}{N}$. Similarly, the objective detection probability is given by

$$F_1(\gamma) = 1-\frac{\Gamma(NM_T, z_1\beta_1)}{\Gamma(NM_T)} \tag{14}$$

with $z_1 = \frac{(\gamma-1)\sigma^2-\mathcal{P}_A\sigma_1^2}{\mathcal{P}_A}$, $\beta_1 = 1-\frac{\sigma_1^2}{N}$. For a specified probability P_f^s, i.e., $P_f^s = 0.1$, the threshold is

$$\gamma = F_0^{-1}\left(\frac{1}{\exp\left(\sqrt[\mu_s]{-\ln P_f^s}\right)}\right), \quad z_0>0, \tag{15}$$

where $F_0^{-1}(\cdot)$ is the inverse function of $F_0(\cdot)$.

B. Ergodic Wiretap Channel Rate

Even if there is a beamforming between Alice and Bob, Eve still can eavesdrop the channel with an ergodic wiretap channel rate $\bar{R}_E$ which is derived by

$$\begin{aligned} \bar{R}_E &= \mathbb{E}\left\{\left[\log\left(1+\frac{\mathcal{P}_A\parallel\hat{\mathbf{h}}_{AE}\parallel^2}{\mathcal{P}_A\tilde{\sigma}_1^2+\sigma^2}\right)\right]^+\right\} \\ &= \ln 2\int_0^\infty \ln\left(1+\frac{\mathcal{P}_A\tilde{\varphi}_1}{\mathcal{P}_A\tilde{\sigma}_1^2+\sigma^2}\right) \\ &\quad\times\tilde{\beta}_1^{M_T}\tilde{\varphi}_1^{M_T-1}\frac{\exp(-\tilde{\beta}_1\tilde{\varphi}_1)}{\Gamma(M_T)}d\tilde{\varphi}_1 \qquad (16) \\ &= \frac{1}{\ln 2}\exp(\mathcal{A})\sum_{k=1}^{M_T}E_k(\mathcal{A}), \qquad (17) \end{aligned}$$

where (17) is the integral form of the ergodic wiretap channel rate, $\tilde{\beta}_1 = 1-\frac{\tilde{\sigma}_1^2}{N}$, $\tilde{\varphi}_1 = \parallel\hat{\mathbf{h}}_{AE}\parallel^2$. $E_k(\cdot)$ is the generalized exponential integral [12], and $\mathcal{A} = \frac{N\mathcal{P}_A\tilde{\sigma}_1^2+N\sigma^2-\mathcal{P}_A\tilde{\sigma}_1^4-\sigma^2\tilde{\sigma}_1^2}{N\mathcal{P}_A}$.

Remark: If the number of samples is big enough at Bob, we can approximately calculate the main channel transmission/secrecy rate using RPNR without any prior channel knowledge, i.e., the channel CSI and the variance of AWGN.

IV. Optimal Spoofing Power And Defense Strategy

When utilizing the RPNR scheme, there is a tradeoff problem for Eve. If Eve adopts higher power to launch the attack, it could greatly increase the ergodic wiretap channel rate. However, higher power increases the probability for Eve being detected. The tradeoff problem can be formulated as

$$\arg\max_{\mathcal{P}_E}(1-P_d^s)\bar{R}_E, \quad \text{s.t. } 0\le\mathcal{P}_E\le\mathcal{P}_e, \tag{18}$$

where $\mathcal{P}_e$ is the power budget constraint at Eve. Substituting (12), (18) into (18), we get

$$\begin{aligned} (1-P_d^s)\bar{R}_E = &\left[1-\exp\left(-\left(\ln\frac{1}{F_1(\gamma)}\right)^{\mu_s}\right)\right] \\ &\times\frac{1}{\ln 2}\exp(\mathcal{A})\sum_{k=1}^{M_T}E_k(\mathcal{A}). \end{aligned} \tag{19}$$

Substituting (3) into (14), and using the strong law of large numbers, we can rewrite (14) as

$$F_1(\gamma) = 1-\frac{\Gamma(NM_T, \dot{z}_1\beta_1)}{\Gamma(NM_T)}, \tag{20}$$

where $\dot{z}_1 = \frac{\mathcal{P}_E(\gamma-1)\sigma^2-\mathcal{P}_A\mathcal{P}_B\tilde{\sigma}_1^2}{\mathcal{P}_A\mathcal{P}_E}$. Substituting (20) into (19), and letting $f(\mathcal{P}_E) = (1-P_d^s)\bar{R}_E$, we note $\frac{d^2}{d^2\mathcal{P}_E}f(\mathcal{P}_E)\ge 0$ (derivation is omitted for brevity), which indicates that $f(\mathcal{P}_E)$ is convex with respect to $\mathcal{P}_E$. To solve the optimal energy transmission strategy $\mathcal{P}_E$ to maximize ergodic wiretap channel rate, we take the derivative of (19) and obtain (22), which is shown at the top of the next page. By setting (22) to be zero and simplifying, we get

$$\frac{\mathcal{P}_E(\gamma-1)\sigma^2-\mathcal{P}_A\mathcal{P}_B\tilde{\sigma}_1^2}{\mathcal{P}_A\mathcal{P}_E} = 0. \tag{23}$$

The solution to (23) is given by $\mathcal{P}_E = \frac{\mathcal{P}_A\mathcal{P}_B\tilde{\sigma}_1^2}{(\gamma-1)\sigma^2}$. Hence, the attacker's optimal power allocation is given by

$$\mathcal{P}_E^* = \begin{cases} \mathcal{P}_e, & \text{if } \mathcal{P}_e < \frac{\mathcal{P}_A\mathcal{P}_B\tilde{\sigma}_1^2}{(\gamma-1)\sigma^2}, \\ \frac{\mathcal{P}_A\mathcal{P}_B\tilde{\sigma}_1^2}{(\gamma-1)\sigma^2}, & \text{if } 0<\frac{\mathcal{P}_A\mathcal{P}_B\tilde{\sigma}_1^2}{(\gamma-1)\sigma^2}<\mathcal{P}_e, \\ 0, & \text{no attacker.} \end{cases} \tag{24}$$

Discussion: Considering the attacker can launch the optimal attack based on the optimal power allocation, we discuss the defense strategy of the optimal attack. From (24), Eve needs the parameters, σ^2, $\mathcal{P}_A$, $\mathcal{P}_B$, γ, to obtain the optimal power allocation. Although σ^2, $\mathcal{P}_A$, $\mathcal{P}_B$ are usually known by Eve, the threshold γ is unknown, especially when Eve locates far away from Bob. Hence, we can keep γ privacy to prevent Eve from launching the optimal attack. However, Eve can utilize a "helper node", which is close to Bob to derive the threshold γ. Even so, we also can defend against the optimal attack through ensuring the confidentiality of the transmission powers. For example, Bob can change the transmission power $\mathcal{P}_B$ in each reverse training phase via a pre-distribution rule only known by Alice, which can prevent Eve from launching the optimal attack. In this case, the ergodic wiretap channel rate $\bar{R}_E$ will be decreased. Since there is no co-channel interference in TDD based channel training, the defense strategy can be extended to the multi-user time division multiple access systems.

V. Simuliations and Performance Analysis

In the simulations, there are multiple-antenna at Alice and single-antenna at Bob and Eve. The probability densities of the RPNR in the presence/absence of attacker are shown in Fig. 1 via 10000 times Monte-Carlo simulations. We verify that the probability densities are different, and the overlapping area represents the false alarm probability P_f and the miss

$$\frac{df(\mathcal{P}_E)}{d\mathcal{P}_E} = \frac{\mu_s}{\ln 2}\exp(\mathcal{A})\sum_{k=1}^{M_T} E_k(\mathcal{A})\exp\left(-(\ln\frac{1}{F_1(\gamma)})^{\mu_s}\right)\left(\ln\frac{1}{F_1(\gamma)}\right)^{\mu_s-1} F_1(\gamma)\frac{\beta_1(\dot{z}_1\beta_1)^{NM_T-1}}{(NM_T-1)!}\exp(-\dot{z}_1\beta_1)\frac{d\dot{z}_1}{d\mathcal{P}_E} \quad (22)$$

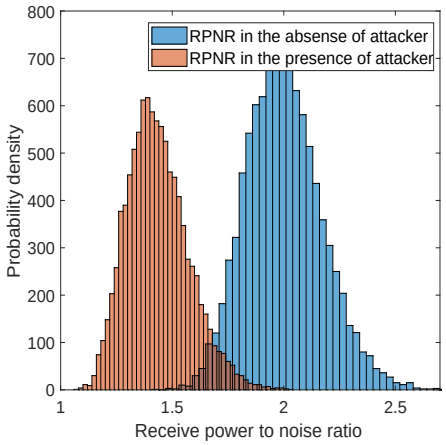

Fig. 1. The probability density of the proposed RPNR scheme.

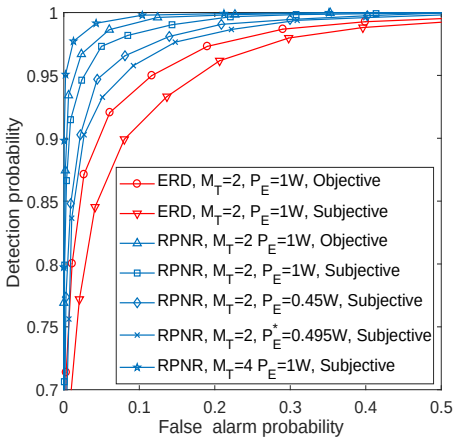

Fig. 2. The ROCs: the ERD [8] vs. the proposed RPNR with different M_T, $\mathcal{P}_E$ and $\mathcal{P}_E^*$.

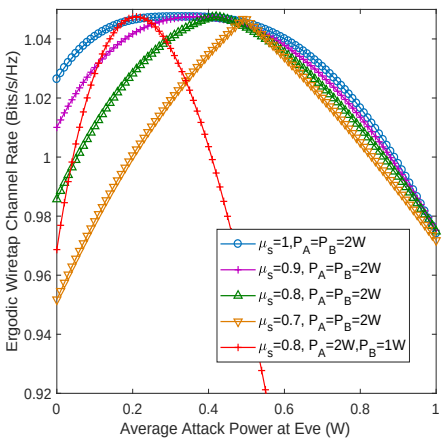

Fig. 3. The spoofing power at Eve with different μ_s, $\mathcal{P}_A$ and $\mathcal{P}_B$.

detection probability $1-P_d$ corresponding to $F_0(\gamma)$ and $F_1(\gamma)$. The approximate bound of the threshold is from 1.5 to 2.

By setting $\mu_s = 1, 0.7$, $M_T = 2, 4$ and $\mathcal{P}_A = \mathcal{P}_B = 2\ W$, for objective/subjective probability, the receiver operating characteristics (ROCs) are shown in Fig. 2. Both the objective and the subjective ROCs show that the proposed RPNR has better detection performance than the ERD method [8]. It is because our proposed scheme can amplify the power gap caused by power leakage, especially in worse channel environment. Interestingly, with $M_T = 2$, the detection performance is improved with the increase of $\mathcal{P}_E$, i.e., $\mathcal{P}_E = 1\ W$ vs. $\mathcal{P}_E = 0.45\ W$, but when the power allocation of Eve is optimal, the detection performance is the worst, i.e., $\mathcal{P}_E = 1\ W$ vs. $\mathcal{P}_E = 0.45\ W$ vs. $\mathcal{P}_E^* = 0.495\ W$. Moreover, the detection performance is improved with M_T increases.

Fig. 3 shows the optimal spoofing power $\mathcal{P}_E^*$ with different subjective parameters μ_s. With $M_T = 2$, $\mathcal{P}_A = \mathcal{P}_B = 2\ W$ and $P_f^s = 0.05$, the optimal spoofing powers are $\mathcal{P}_E^* = \{0.495\ W, 0.420\ W, 0.366\ W, 0.327\ W\}$ corresponding to $\mu_s = \{0.7, 0.8, 0.9, 1\}$. It suggests that the optimal spoofing power $\mathcal{P}_E^*$ increases with μ_s decreases. We find that a large range of potential spoofing power $\mathcal{P}_E$ stays close to the optimal spoofing power $\mathcal{P}_E^*$. That is, the bigger the subjective parameter μ_s is, the larger range it is. We conclude that the proposed subjective probability can increase the system's robustness and mitigate the power leakage. When $\mathcal{P}_B$ changes from $2\ W$ to $1\ W$, the optimal spoofing power $\mathcal{P}_E^*$ changes from $0.420\ W$ to $0.2098\ W$, which shows that the optimal attack cannot be launched by the attacker without knowing $\mathcal{P}_B$ and the ergodic wiretap channel rate $\bar{R}_E$ will be decreased.

VI. Conclusion

We have redefined the subjective probability by considering the prior uncertainty of the attack. A detection scheme has been proposed based on the received power-to-noise ratio. We have analyzed the tradeoff problem between the ergodic wiretap channel rate and the subjective detection probability, and derived the attacker's optimal power allocation. Besides, we have discussed the defense strategy of the optimal attack. Simulations have validated the proposed scheme.

References

[1] Y. Alsaba, S. K. A. Rahim, and C. Y. Leow, "Beamforming in wireless energy harvesting communications systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1329–1360, 2nd Quart. 2018.

[2] B. Akgun, M. Krunz, and O. O. Koyluoglu, "Vulnerabilities of massive MIMO systems to pilot contamination attacks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1251–1263, May 2019.

[3] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. on Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[4] K. Yuan, L. Guo, C. Dong, and T. Kang, "Detection of active eavesdropper using source enumeration method in massive MIMO," in *Proc. IEEE ICC*, May 2017, pp. 1–5.

[5] D. Xu, P. Ren, J. A. Ritcey, and Y. Wang, "Code-frequency block group coding for anti-spoofing pilot authentication in multi-antenna OFDM systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1778–1793, Jul. 2018.

[6] J. K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 525–528, Oct. 2015.

[7] ——, "Pilot spoofing attack detection and countermeasure," *IEEE Trans. on Commun.*, vol. 66, no. 5, pp. 2093–2106, May 2018.

[8] Q. Xiong, Y. C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[9] S. M. Kay, "Fundamentals of statistical signal processing, volume I: estimation theory," 1993.

[10] E. Telatar, "Capacity of multi-antenna gaussian channels," *Trans. Emerg. Telecommun. Tech.*, vol. 10, no. 6, pp. 585–595, Nov. 1999.

[11] D. Prelec, "The probability weighting function," *Econometrica*, vol. 66, no. 3, pp. 497–527, May 1998.

[12] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. New York: Academic Press, 2014.